C

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/602,696	06/25/2003	Makoto Aikawa	501.42780X00	1583

24956 7590 01/10/2007
MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
GERGISO, TECHANE	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/602,696	**Applicant(s)** AIKAWA ET AL.	
	Examiner Techane J. Gergiso TG	**Art Unit** 2137	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *07/07/03;06/25/03;* .

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This is a non-final Office Action in response to the applicant's election filed on October 23, 2006.

2. The applicant elected group I (claims 1, 3, 5, and 8) without traverse for restriction requirement mailed on September 28, 2006.

3. Claims 1-9 have been examined.

4. Claims 1-9 are pending.

Specification

5. The disclosure filed on June 25, 2003 is objected to because of the following informalities:

The application has several hand written editing words and phrases throughout the disclosure; which most of them are not clear and readable. Clear printed copy of the disclosure and appropriate correction is required.

The disclosure provides only page numbers (pages 1-61). There are no line numbers or paragraph numbers designated to each paragraph throughout the disclosure which to cite from the disclosure. Each and every paragraph requires to be renumbered and appropriate correction is required.

6. A substitute specification including the claims is required pursuant to 37 CFR 1.125(a) because.

The application has several hand written editing words and phrases throughout the disclosure; which most of them are not clear and readable. Clear printed copy of the disclosure and appropriate correction is required and the disclosure provides only page numbers (pages 1-61). There are no line numbers or paragraph numbers designated to each paragraph throughout the disclosure which to cite from the disclosure. Each and every paragraph requires to be renumbered and appropriate correction is required.

A substitute specification must not contain new matter. The substitute specification must be submitted with markings showing all the changes relative to the immediate prior version of the specification of record. The text of any added subject matter must be shown by underlining the added text. The text of any deleted matter must be shown by strike-through except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived. An accompanying clean version (without markings) and a statement that the substitute specification contains no new matter must also be supplied. Numbering the paragraphs of the specification of record is not considered a change that must be shown.

7. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: **Secure Data Transfer between Two Smart Cards.**

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term "**update**" in claim 1-9 are used by the claim to mean "**encryption**", while the accepted meaning is **"To change a system or a data file to make it more current." (See Microsoft Computer Dictionary).** The term is indefinite because the specification does not clearly redefine the term.

11. Regarding claims 1, 3, 5 and 8; the phrase "**used to update**" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

12. Regarding claims 1, 3, and 5; the phrase "**used to judge**" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

13. Regarding claim 8, the phrase "**used to identify**" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

14. Claim 1, 3, 5 and 8 recites the limitation "then" in "said arithmetic processing unit **then** updates the value data ...." The word "**then**" in the claims suggest or implies that the action of **updating** is a followed from or based on a previously carried out action which the claims do not clear and specifically recite such previous action. There is insufficient antecedent basis for this limitation in the claim.

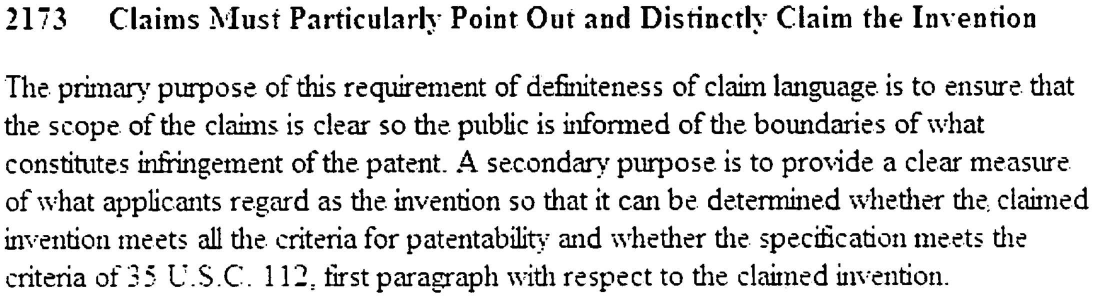
15. The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

Fore example **the third limitation in claim 4 reads and it is not clear to what extent it determines the scope of the claim**:

"if command data which requests update of the transfer key, and which stores second encrypted data and second digital signature data, is received, first checking the second digital signature data by use of the second public key on the basis of public-key cryptography, next decrypting the second encrypted data by use of the secret key on the basis of public-key cryptography to extract first data and second data, and lastly if a value of the first data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the first data, and updating a value of the transfer key to a value of the second data;"

The limitations in the claims are required to be rewritten to provide in a clear and precise language to determine the scope and boundaries of the claimed invention.

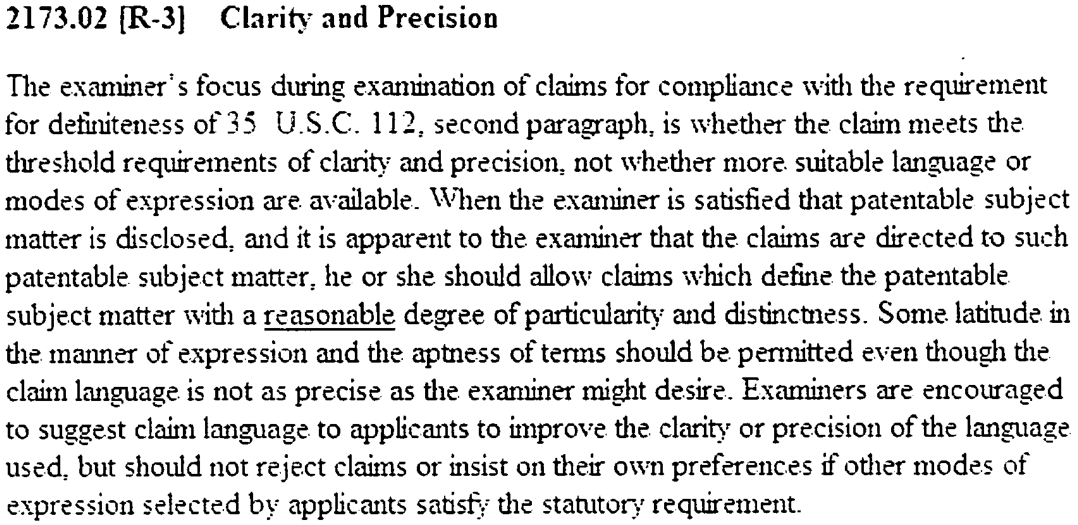
See MPEP



2173 Claims Must Particularly Point Out and Distinctly Claim the Invention

The primary purpose of this requirement of definiteness of claim language is to ensure that the scope of the claims is clear so the public is informed of the boundaries of what constitutes infringement of the patent. A secondary purpose is to provide a clear measure of what applicants regard as the invention so that it can be determined whether the claimed invention meets all the criteria for patentability and whether the specification meets the criteria of 35 U.S.C. 112, first paragraph with respect to the claimed invention.

and



2173.02 [R-3] Clarity and Precision

The examiner's focus during examination of claims for compliance with the requirement for definiteness of 35 U.S.C. 112, second paragraph, is whether the claim meets the threshold requirements of clarity and precision, not whether more suitable language or modes of expression are available. When the examiner is satisfied that patentable subject matter is disclosed, and it is apparent to the examiner that the claims are directed to such patentable subject matter, he or she should allow claims which define the patentable subject matter with a reasonable degree of particularity and distinctness. Some latitude in the manner of expression and the aptness of terms should be permitted even though the claim language is not as precise as the examiner might desire. Examiners are encouraged to suggest claim language to applicants to improve the clarity or precision of the language used, but should not reject claims or insist on their own preferences if other modes of expression selected by applicants satisfy the statutory requirement.

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 1, 3, 5, and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guthery (US Pat No: 6, 779, 113) in view of Akiyama et al. (hereinafter referred to as Akiyama, US Pat. No.: 6, 018, 717).

As per claim 1:

Guthery disclose a smart card (figure 2: 26; IC Card), comprising:

communication unit to communicate with the outside (figure 2: 50; Reader Interface);

information accumulating unit to accumulate data and a program (figure 2: 54; RAM; 56);

arithmetic processing unit to perform information processing (figure 2: 52 CPU, Cryptography Accelerator; 62);

wherein:

said information accumulating unit stores value data, a transfer key used to update the value data, a transfer key identifier used to judge whether the transfer key is newer or older in accordance with a value of the transfer key identifier, an update key used to update the transfer key, and an upper limit of transfer key identifier that represents an upper limit of the transfer key identifier that can be stored by the smart card (Column 5: lines 27-42; Column 6: lines 60-67; column 7: line 1-5; column 12: lines 1-25);

said arithmetic processing unit updates the transfer key identifier and the transfer key by performing encryption using the update key on the basis of common-key cryptography (column 7: lines 39-45); and

said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of the common-key cryptography (column 7: lines 39-45).

Guthery does not disclose update value data. Akiyama, in analogous art, however, discloses updating transaction and update value data (Figure 15: IC card ledger file). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery to include updating transaction and update value data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an enhanced security of an electronic cashless transaction system, thereby allowing versatile uses of an IC card as an ultimate medium for commercial transactions in general as suggested by Akiyama in (column 4: lines 43-48).

As per claim 3:

Guthery disclose a smart card, comprising:

communication unit to communicate with the outside (figure 2: 26; IC Card);

information accumulating unit to accumulate data and a program (figure 2: 54; RAM; 56); and

arithmetic processing unit to perform information processing (figure 2: 52 CPU, Cryptography Accelerator; 62); wherein:

said information accumulating unit stores value data, a transfer key used to update the value data, a transfer key identifier used to judge whether the transfer key is newer or older in accordance with a value of the transfer key identifier, a first public key certificate including a first public key, which is used to update the transfer key, a secret key corresponding to the first public key, and an upper limit of transfer key identifier that represents an upper limit of the transfer key identifier which can be stored by the smart card (Column 5: lines 27-42; Column 6: lines 60-67; column 7: line 1-5; column 12: lines 1-25);

said arithmetic processing unit updates the transfer key identifier and the transfer key by performing encryption using the first public key certificate and the secret key on the basis of public-key cryptography (column 7: lines 39-45); and

said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of common-key cryptography (column 7: lines 39-45).

Guthery does not disclose update value data. Akiyama, in analogous art, however, discloses updating transaction and update value data (Figure 15: IC card ledger file). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery to include updating transaction and update value data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an enhanced security of an electronic cashless transaction system, thereby allowing versatile uses of an IC card as an ultimate medium for commercial transactions in general as suggested by Akiyama in (column 4: lines 43-48).

As per claim 5:

Guthery disclose a smart card, comprising:

communication unit to communicate with the outside (figure 2: 26; IC Card);

information accumulating unit to accumulate data and a program (figure 2: 54; RAM; 56); and arithmetic processing unit to perform information processing (figure 2: 52 CPU, Cryptography Accelerator; 62);

wherein:

said information accumulating unit stores value data, a transfer key used to update the value data, a transfer key identifier used to judge whether the transfer key is newer or older in accordance with a value of the transfer key identifier, an update key used to update the transfer key, an update key identifier used to judge whether the update key is newer or older in accordance with a value of the update key identifier, a first public key certificate including a first public key, which is used to update the transfer key, a secret key corresponding to the first public key, and an upper limit of transfer key identifier that represents an upper limit of the transfer key identifier which can be stored by the smart card (Column 5: lines 27-42; Column 6: lines 60-67; column 7: line 1-5; column 12: lines 1-25);

said arithmetic processing unit updates the transfer key by use of the update key on the basis of common-key cryptography, or updates the transfer key by use of the first public key certificate and the secret key on the basis of common-key cryptography (column 7: lines 39-45); and

said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of the common-key cryptography (column 7: lines 39-45).

Guthery does not disclose update value data. Akiyama, in analogous art, however, discloses updating transaction and update value data (Figure 15: IC card ledger file). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery to include updating transaction and update value data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an enhanced security of an electronic cashless transaction system, thereby allowing versatile uses of an IC card as an ultimate medium for commercial transactions in general as suggested by Akiyama in (column 4: lines 43-48).

As per claim 8:

Guthery disclose a smart card, comprising:

communication unit to communicate with the outside (figure 2: 26; IC Card);

information accumulating unit to accumulate data and a program (figure 2: 54; RAM; 56); and

arithmetic processing unit to perform information processing (figure 2: 52 CPU, Cryptography Accelerator; 62);

wherein:

said information accumulating unit stores value data, one or more transfer keys used to update the value data, a selection transfer key identifier used to identify the transfer key currently selected, and an update key used to update the transfer key (Column 5: lines 27-42; Column 6: lines 60-67; column 7: line 1-5; column 12: lines 1-25);

said arithmetic processing unit updates the selection transfer key identifier by performing encryption using the update key on the basis of common-key cryptography (column 7: lines 39-45); and

said arithmetic processing unit then updates the value data by performing encryption using the transfer key on the basis of common-key cryptography (column 7: lines 39-45).

Guthery does not disclose update value data. Akiyama, in analogous art, however, discloses updating transaction and update value data (Figure 15: IC card ledger file). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery to include updating transaction and update value data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an enhanced security of an electronic cashless transaction system, thereby allowing versatile uses of an IC card as an ultimate medium for commercial transactions in general as suggested by Akiyama in (column 4: lines 43-48).

18. Claims 2, 4, 6, 7 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guthery (US Pat No: 6, 779, 113) in view of Akiyama et al. (hereinafter referred to as Akiyama, US Pat. No.: 6, 018, 717) and further in view of Richards et al.(hereinafter referred to as Richards, US Pat No.: 6,230,267).

As per claim 2:

Guthery disclose a smart card according, wherein said arithmetic processing unit comprises the steps of:

if command data that requests transmission of card information is received, transmitting the transfer key identifier to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16);

if command data that requests update permission of the transfer key is received, generating a first random number and transmitting the first random number to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16); and

if the command data which requests to obtain the transfer key, and which stores a second random number, is received, transmitting first encrypted data, into which the second random number, the transfer key identifier, and the transfer key are encrypted by use of the update key on the basis of common-key cryptography, to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16).

Guthery and Akiyama do not disclose if command data which requests update of the transfer key, and which stores second encrypted data, is received, decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and if the first data is equivalent to the first random number, and if a value of the second data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the second data, and updating a value of the transfer key to a value of the third data.

Richards, in analogous art, however, discloses if command data which requests update of the transfer key, and which stores second encrypted data, is received, decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and if the first data is equivalent to the first random number, and if a value of the second data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the second data, and updating a value of the transfer key to a value of the third data (column 9: lines 10-43; column 11: lines 14-30).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery and Akiyama to include if command data which requests update of the transfer key, and which stores second encrypted data, is received, decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and if the first data is equivalent to the first random number, and if a value of the second data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the second data, and updating a value of the transfer key to a value of the third data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an IC card method and apparatus for securely transporting data including an application onto an IC card including storing a secret and public key pair on the IC card, retrieving the stored public key from the IC card, encrypting at least a portion of the data to be transported using the public key, transmitting the encrypted data to the IC card and decrypting the encrypted data using the IC card's secret key as suggested Richards in (Column 2: lines 45-62).

As per claim 4:

Guthery disclose a smart card, wherein:

said arithmetic processing unit comprises the steps of:

if command data that requests transmission of card information is received, transmitting the transfer key identifier and the first public key certificate to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16; figure 2: 78, 80);

if command data which requests update permission of the transfer key, and which stores a second public key certificate including a second public key, is received, generating a first random number and transmitting the first random number to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16); and

if command data which requests update of the transfer key, and which stores second encrypted data and second digital signature data, is received, first checking the second digital signature data by use of the second public key on the basis of public-key cryptography, next decrypting the second encrypted data by use of the secret key on the basis of public-key cryptography to extract first data and second data, and lastly if a value of the first data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the first data, and updating a value of the transfer key to a value of the second data (column 7: lines 29-45; column 9: lines 24-56).

Guthery and Akiyama do not disclose if command data which requests to obtain the transfer key, and which stores a second random number and a third public key certificate including a third public key, is received, first creating first encrypted data into which the transfer key identifier and the transfer key are encrypted by use of the third public key on the basis of public-key cryptography, next creating first digital signature data from the first encrypted data and the second random number by use of the secret key on the basis of public-key cryptography, and lastly transmitting the first encrypted data and the first digital signature data to the outside as response data.

Richards, in analogous art, however, discloses if command data which requests to obtain the transfer key, and which stores a second random number and a third public key certificate including a third public key, is received, first creating first encrypted data into which the transfer key identifier and the transfer key are encrypted by use of the third public key on the basis of public-key cryptography, next creating first digital signature data from the first encrypted data and the second random number by use of the secret key on the basis of public-key cryptography, and lastly transmitting the first encrypted data and the first digital signature data to the outside as response data (column 9: lines 10-43; column 11: lines 14-30; figure 3: 90, 92, 94; column 14: lines 35-65).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery and Akiyama to include if command data which requests to obtain the transfer key, and which stores a second random number and a third public key certificate including a third public key, is received, first creating first encrypted data into which the transfer key identifier and the transfer key are encrypted by use of the third public key on the basis of public-key cryptography, next creating first digital signature data from the first encrypted data and the second random number by use of the secret key on the basis of public-key cryptography, and lastly transmitting the first encrypted data and the first digital signature data to the outside as response data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an IC card method and apparatus for securely transporting data including an application onto an IC card including storing a secret and public key pair on the IC card, retrieving the stored public key from the IC card, encrypting at least a portion of the data to be transported using the public key, transmitting the encrypted data to the IC card and decrypting the encrypted data using the IC card's secret key as suggested Richards in (Column 2: lines 45-62).

As per claim 6:

Guthery disclose a smart card, wherein:

said arithmetic processing unit comprises the steps of:

if command data that requests transmission of card information is received, transmitting the transfer key identifier, the update key identifier, and the first public key certificate to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16; figure 2: 78, 80);

if command data that requests update permission of the transfer key is received, generating a first random number and transmitting the first random number to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16); and

if the command data which requests to obtain the transfer key, and which stores a second random number, is received, transmitting first encrypted data, into which the second random number, the transfer key identifier, and the transfer key are encrypted by use of the update key on the basis of common-key cryptography, to outside as response data (column 7: lines 29-45; column 9: lines 24-56).

Guthery and Akiyama do not disclose if command data which requests update of the transfer key, and which stores second encrypted data, is received, first decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and next if the first data is equivalent to the first random number, and if a value of the second data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the second data, and updating a value of the transfer key to a value of the third data.

Richards, in analogous art, however, discloses if command data which requests update of the transfer key, and which stores second encrypted data, is received, first decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and next if the first data is equivalent to the first random number, and if a value of the second data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the second data, and updating a value of the transfer key to a value of the third data (column 9: lines 10-43; column 11: lines 14-30; figure 3: 90, 92, 94; column 14: lines 35-65).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery and Akiyama to include if command data which requests update of the transfer key, and which stores second encrypted data, is received, first decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and next if the first data is equivalent to the first random number, and if a value of the second data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the second data, and updating a value of the transfer key to a value of the third data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an IC card method and apparatus for securely transporting data including an application onto an IC card including storing a secret and public key pair on the IC card, retrieving the stored public key from the IC card, encrypting at least a portion of the data to be transported using the public key, transmitting the encrypted data to the IC card and decrypting the encrypted data using the IC card's secret key as suggested Richards in (Column 2: lines 45-62).

As per claim 7:

Guthery disclose a smart card, wherein:

said arithmetic processing unit comprises the steps of:

if command data that requests transmission of card information is received, transmitting the transfer key identifier, the update key identifier, and the first public key certificate to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16; figure 2: 78, 80);

if command data which requests update permission of the transfer key, and which stores a second public key certificate including a second public key, is received, generating a first random number and transmitting the first random number to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16); and

if command data which requests to obtain the transfer key, and which stores a second random number and a third public key certificate including a third public key, is received, first creating first encrypted data into which the transfer key identifier and the transfer key are encrypted by use of the third public key on the basis of public-key cryptography, next creating first digital signature data from the first encrypted data and the second random number by use of the secret key on the basis of public-key cryptography, and lastly transmitting the first encrypted data and the first digital signature data to outside as response data (column 7: lines 29-45; column 9: lines 24-56).

Guthery and Akiyama do not disclose if command data which requests update of the transfer key, and which stores second encrypted data and second digital signature data, is received, first checking the second digital signature data by use of the second public key on the basis of public-key cryptography, next decrypting the second encrypted data by use of the secret key on the basis of public-key cryptography to extract first data and second data, and lastly if a value of the first data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the first data, and updating a value of the transfer key to a value of the second data.

Richards, in analogous art, however, discloses if command data which requests update of the transfer key, and which stores second encrypted data and second digital signature data, is received, first checking the second digital signature data by use of the second public key on the basis of public-key cryptography, next decrypting the second encrypted data by use of the secret key on the basis of public-key cryptography to extract first data and second data, and lastly if a value of the first data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the first data, and updating a value of the transfer key to a value of the second data. (column 9: lines 10-43; column 11: lines 14-30; figure 3: 90, 92, 94; column 14: lines 35-65).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery and Akiyama to include if command data which requests update of the transfer key, and which stores second encrypted data and second digital signature data, is received, first checking the second digital signature data by use of the second public key on the basis of public-key cryptography, next decrypting the second encrypted data by use of the secret key on the basis of public-key cryptography to extract first data and second data, and lastly if a value of the first data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updating a value of the transfer key identifier to a value of the first data, and updating a value of the transfer key to a value of the second data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an IC card method and apparatus for securely transporting data including an application onto an IC card including storing a secret and public key pair on the IC card, retrieving the stored public key from the IC card, encrypting at least a portion of the data to be transported using the public key, transmitting the encrypted data to the IC card and decrypting the encrypted data using the IC card's secret key as suggested Richards in (Column 2: lines 45-62).

As per claim 9:

Guthery disclose a smart card according to claim 8, wherein:

said arithmetic processing unit comprises the steps of:

if command data that requests transmission of card information is received, transmitting the selection transfer key identifier to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16; figure 2: 78, 80);

if command data that requests update permission of the transfer key is received, generating a first random number and transmitting the first random number to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16); and

if the command data which requests to obtain the transfer key, and which stores a second random number, is received, transmitting first encrypted data, into which the second random number, the selection transfer key identifier, and the transfer key are encrypted by use of the update key on the basis of common-key cryptography, to the outside as response data (Column 15: lines 40-65; Column 16: lines 1-16).

Guthery and Akiyama do not disclose if command data which requests update of the transfer key, and which stores second encrypted data, is received, decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and if the first data is equivalent to the first random number, and if a value of the second data is equivalent to one of values of the transfer key identifiers, updating a value of the selection transfer key identifier to a value of the second data.

Richards, in analogous art, however, discloses if command data which requests update of the transfer key, and which stores second encrypted data, is received, decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and if the first data is equivalent to the first random number, and if a value of the second data is equivalent to one of values of the transfer key identifiers, updating a value of the selection transfer key identifier to a value of the second data (column 9: lines 10-43; column 11: lines 14-30; figure 3: 90, 92, 94; column 14: lines 35-65).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Guthery and Akiyama to include if command data which requests update of the transfer key, and which stores second encrypted data, is received, decrypting the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and if the first data is equivalent to the first random number, and if a value of the second data is equivalent to one of values of the transfer key identifiers, updating a value of the selection transfer key identifier to a value of the second data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide an IC card method and apparatus for securely transporting data including an application onto an IC card including storing a secret and public key pair on the IC card, retrieving the stored public key from the IC card, encrypting at least a portion of the data to be transported using the public key, transmitting the encrypted data to the IC card and decrypting the encrypted data using the IC card's secret key as suggested Richards in (Column 2: lines 45-62).

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art

Contact Information

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T·G

Techane Gergiso

Patent Examiner

Art Unit 2137

January 3, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER